APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,454	02/26/2004	Sarvar Patel	29250-002013/US	4912

7590   01/03/2012

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 8910
Reston, VA 20195

EXAMINER
TOLENTINO, RODERICK

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/03/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/786,454
Filing Date: February 26, 2004
Appellant(s): PATEL ET AL.

Gary Yacura (35,416)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/3/2011 appealing from the Office action

mailed 6/03/2011.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying

by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial

proceedings which will directly affect or be directly affected by or have a bearing on the

Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

1 – 24 are pending.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of

amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter

contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of

rejection to be reviewed on appeal. Every ground of rejection set forth in the Office

action from which the appeal is taken (as modified by any advisory actions) is being

maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are

provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in

the Appendix to the appellant's brief.

(8) Evidence Relied Upon

2005/0086468	Meanddzija	04-2005
2004/0078334	Malcolm et al.	04-2004
2005/0172116	Burch et al.	08-2005
2005/0177715	Somin et al.	08-2005
6,980,658	Rezaiifar et al.	11-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 4, 6, 7, 11 and 12 are are rejected under 35 U.S.C. 103(a) as being

unpatentable over Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of

Malcolm et al. U.S. PG-Publication No. (2004/0078334).

As per claims 1, Meandzija teaches the first cryptosync having a life limited to the

communication session, the comnmnication session being defined as a period of time a

channel for communication exists between the two communication devices (Meandzija,

Paragraph 0073, session certificate which is only valid for a single session) but fails to

teach deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync and the second cryptosync having a life extending over multiple communication sessions. However, in an analogous art Malcolm teaches deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate) and the second cryptosync having a life extending over multiple communication sessions (Malcolm, Paragraph 0145, certificate derived from root certificate, the root certificate is being interpreted to be the second cryptosync which will last over multiple sessions since all the signed certificates will stem from the root).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Malcolm's Information management system Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of ensuring that the transmission of data by their staff is always carried out securely (Malcolm, Paragraph 0028).

As per claim 4, Meandzija as modified teaches the second cryptosync is used for verifying message integrity by at least one of the two devices (Meandzija, Paragraph 0007, communications between user terminal and access points).

As per claim 6, Meandzija as modified teaches deriving step derives the first cryptosync as at least a portion of the second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate).

As per claim 7, Meandzija as modified teaches the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence (Malcolm, Paragraph 0145, certificate derived from root certificate).

As per claim 11, Meandzija as modified teaches the deriving step derives a portion of the first cryptosync as the second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate).

As per claim 12, Meandzija as modified teaches the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence (Malcolm, Paragraph 0145, certificate derived from root certificate).

Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meandzija et al. U.S. PG-Publication No. (2005/0086468) and Malcolm et al. U.S. PG-Publication No. (2004/0078334) in view of Burch et al. U.S. PG-Publication No. (2005/0172116).

As per claim 2, Meandzija fails to teach the second cryptosync is used for message encryption by at least one of the two devices. However in an analogous art Burch teaches the second cryptosync is used for message encryption by at least one of the two devices (Burch, Paragraphs 0004 and 0023, certificate encrypts communications).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Burch's techniques for dynamically establishing and

managing trust relationships with Meandzija's digital certificate related to the user

terminal hardware in a wireless network because it offers the advantage of improving

trust relationships (Burch, Paragraph 0008).

As per claim 3, Meandzija as modified teaches the second cryptosync is used for

verifying message integrity by at least one of the two devices (Meandzija, Paragraph

0007, communications between user terminal and access points).

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et

al. U.S. PG-Publication No. (2004/0078334) and Somin et al. U.S. PG-Publication No.

(2005/0177715)

As per claim 5, Meandzija fails to teach the second cryptosync changes between

communication sessions. However, in an analogous art Somin teaches the second

cryptosync changes between communication sessions (Somin, Paragraph 0043, new

root certificate needed).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Somin's system for managing identities with Meandzija's

digital certificate related to the user terminal hardware in a wireless network because it

offers the advantage of effectively resolve the communications issues of addressing,

identity verification, and trust extension (Somin, Paragraph 0007).

Claims 8 – 10 and 13 – 23 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of

Malcolm et al. U.S. PG-Publication No. (2004/0078334) in further view of Rezaiifar et al.

U.S. Patent No. (6,980,658).

As per claim 8, Meandzija fails to teach the deriving step derives most significant

bits of the first cryptosync as the portion of the second cryptosync and derives least

significant bits of the first cryptosync as the fixed bit sequence. However, in an

analogous art Rezaiifat teaches the deriving step derives most significant bits of the first

cryptosync as the portion of the second cryptosync and derives least significant bits of

the first cryptosync as the fixed bit sequence (Rezaiifar, Col. 4 Lines 46 – 62, bit

sequence).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art, to use Rezaiifar's method and apparatus for encrypting

transmissions in a communication system with Meandzija's digital certificate related to

the user terminal hardware in a wireless network because it offers the advantage of

maintaining encryption protocols to prevent the disclosure of communications between

parties (Rezaiifar, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 2).

As per claim 9, Meandzija as modified teaches the fixed bit sequence is a string

of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

As per claim 10, Meandzija as modified teaches the deriving step derives a 32

most significant bits of the first cryptosync as the second cryptosync and derives a 32

least significant bits of the first cryptosync as a string of 0s (Rezaiifar, Col. 9 Lines 11 –

22, EID value of Zero).

As per claim 13, Meandzija as modified teaches the fixed bit sequence is a string

of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

As per claim 14, Meandzija as modified teaches the deriving step comprises:

performing a pseudo-random function on the second cryptosync; and generating the

first cryptosync from output of the pseudo-random function (Rezaiifar, Col. 8 Lines 15 –

21, randomly chosen).

As per claim 15, Meandzija as modified teaches the generating step generates

the first cryptosync as the output of the pseudo-random function (Rezaiifar, Col. 8 Lines

15 – 21, randomly chosen).

As per claim 16, Meandzija as modified teaches the deriving step is performed at

a base station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).

As per claim 17, Meandzija as modified teaches the deriving step is performed at

a mobile station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).

As per claim 18, Meandzija as modified teaches encrypting a frame of

information to send from the at least one of the two devices using the first cryptosync

(Rezaiifar, Col. 2 Lines 19 – 23, encryption).

As per claim 19, Meandzija as modified teaches the frame of information is a

radio link protocol, RLP, frame (Rezaiifar, Col. 6 Lines 45 – 56, RLP frames).

As per claim 20, Meandzija as modified teaches incrementing the first cryptosync

after the encrypting step (Rezaiifar, Col. 2 Lines 38 - 48, incrementing).

As per claim 21, Meandzija as modified teaches decrypting a frame of information received at the at least one of the two devices using the first cryptosync (Rezaiifar, Col. 5 Lines 56 – 67, decryption).

As per claim 22, Meandzija as modified teaches the frame of information is a radio link protocol, RLP, frame (Rezaiifar, Col. 6 Lines 45 – 56, RLP frames).

As per claim 23, Meandzija as modified teaches incrementing the first cryptosync after the decrypting step (Rezaiifar, Col. 2 Lines 38 – 48, incrementing).

Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et al. U.S. PG-Publication No. (2004/0078334) and Burch et al. U.S. PG-Publication No. (2005/0172116).

As per claim 24, Meandzija teaches the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices (Meandzija, Paragraph 0073, session certificate which is only valid for a single session) but fails to teach deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync and the second cryptosync having a life extending over multiple communication sessions and [cryptosync] used to encrypt further communication between the two devices. However, in an analogous art Malcolm teaches deriving, at a network element, a value of a first cryptosync for the

communication session based on a value of a second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate) and the second cryptosync having a life extending over multiple communication sessions (Malcolm, Paragraph 0145, certificate derived from root certificate, the root certificate is being interpreted to be the second cryptosync which will last over multiple sessions since all the signed certificates will stem from the root) and Burch teaches [cryptosync] used to encrypt further communication between the two devices (Burch, Paragraphs 0004 and 0023, certificate encrypts communications).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Malcolm's Information management system Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of ensuring that the transmission of data by their staff is always carried out securely (Malcolm, Paragraph 0028).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Burch's techniques for dynamically establishing and managing trust relationships with Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of improving trust relationships (Burch, Paragraph 0008).

(10) Response to Argument

Response to Section A, Regarding Claim 5:

Examiner withdraws 112 rejection of claim 5. Arguments from Appellant regarding this rejection only have been deemed persuasive.

Response to Section B, Regarding Claim 1:

Appellant argues that Meandzija in view of Malcolm fail to disclose, teach or even suggest "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions," regarding claim 1. Examiner respectfully disagrees.

Claim 1 can be essentially broken down into two parts. The first part is "the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices," which Examiner relies upon Meandzija to teach this. This portion of recited limitation is claiming a cryptosync. A cryptosync in the broadest interpretation is a piece of cryptographic information; this could be anything from a counter, to an encryption key or a digital certificate or a number of other pieces of information. A public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. With the interpretation that a cryptosync can be a digital certificate the

Examiner relies on the prior art of Meandzija to teach this first portion of claim 1.

Meandzija teaches the use of digital certificates in a wireless access network which are

used to enable user terminals to authenticate themselves with access points in the

network. Paragraph 0018 of Meandzija teaches how these access points and user

terminals communicate wirelessly with each other when a user connects to the network.

Examiner would like to focus on Paragraphs 0071 – 0073 of Meandzija. In these

paragraphs Meandzija teaches the use of session certificates. These session

certificates are still considered digital certificates. These being session certificates are

only good for use one session, as taught by Meandzjia on paragraph 0073. This

teaches the first recited portion of claim 1 by showing that the digital certificate is not

permanent since it is a session certificate. The session certificates are used for

communication between two communication devices, which are the wireless network

access point and the user terminal which is described to be a PDA, laptop etc. All

limitations of the first portion of recited claim 1 are taught by Meandzija.

The second part is "deriving, at a network element, a value of a first cryptosync

for the communication session based on a value of a second cryptosync, the second

cryptosync having a life extending over multiple communication sessions," which the

Examiner has used Malcolm to teach in combination with Meandzija. This portion of

recited limitation is focused on a second cryptosync. As taught above a cryptosync is

being interpreted to be a digital signature. The first portion is discussing a first

cryptosync, and this second portion is talking about the creation/derivation of that

cryptosync. Malcolm teaches an information system that allows a user connect to the

network which is synonymous with Meandzija's reference which connects a user

terminal and an access point which is part of a wireless network. Also synonymous to

Meandzija is Malcolm's use of digital certificates, which are used to validate a user and

allow them access to the network or deny them access to a network if a certificate is

invalid. Examiner has used Malcolm to teach the creation of a digital certificate.

Paragraph 0145 or Malcolm teaches a Certificate Authority. A certificate authority, is an

entity that issues digital certificates. The digital certificate certifies the ownership of a

public key by the named subject of the certificate. Meanddzija teaches that certificate

authorities are needed to issue certificates, in their reference, these include session

certificates. Now, Malcolm on paragraph 0145 teaches a certificate authority which

issues digital certificates. Each digital certificate created maybe derived from a root

certificate. A certificate authority can issue multiple certificates in the form of a tree

structure. A root certificate is the top-most certificate of the tree, the private key of

which is used to "sign" other certificates. All certificates immediately below the root

certificate inherit the trustworthiness of the root certificate - a signature by a root

certificate is somewhat analogous to "notarizing" an identity in the physical world.

Certificates further down the tree also depend on the trustworthiness of the

intermediates (often known as "subordinate certification authorities"). What this

essentially teaches is that any certificate is derived from this root certificate since all are

linked back to the root if you follow the tree structure. To read on the recited limitation

of this second portion of claim 1, the root certificate is the second cryptosync in which a

first cryptosync is derived. The combination of with Meandzija and Malcolm, will teach a

certificate authority which creates session certificates, which are digital certificates, and

that each certificate is derived from the certificate authorities root certificate. The root

certificate will always derive new certificates so it will have a lifespan that will be longer

than any session certificate it creates. This reads on the limitation the a the root

certificate being the second cryptostync will last over multiple communication sessions.

In response to appellant's argument that there is no teaching, suggestion, or

motivation to combine the references, the examiner recognizes that obviousness may

be established by combining or modifying the teachings of the prior art to produce the

claimed invention where there is some teaching, suggestion, or motivation to do so

found either in the references themselves or in the knowledge generally available to one

of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir.

1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR*

International Co. v. Teleflex, Inc., 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case,

both the Meandzija and Malcolm are analogous art. Both references deal with the use

of digital certificates used to connect to a network and a user terminal in secure

communication. Malcolm teaches a specific certificate authority that creates digital

signatures that are derived from a root certificate. Meandzija teaches the use of

session certificates, which are valid for one communication session, to connect a user

terminal and a network access point. Combining the two references teaches the system

used for having communication sessions between a network and user terminal, wherein

digital certificates are synonymous with cryptosyncs and are used to help connecting

the user terminal and network, and the certificates do not last forever and a derived

from a root certificate at the certificate authority. The advantage of combining Malcolm

with Meandzija is to have secure communications during a session. Evidence for this

is shown in paragraph 0028 where it teaches the need for the secure transmission of

data in a communication.

Response to Section B, Regarding Claim 4:

Appellant argues that Meandzija in view of Malcolm fail to disclose, teach or even

suggest "wherein the second cryptosync is used for verifying message integrity by at

least one of the two devices," regarding claim 4. Examiner respectfully disagrees.

Meandzija as modified teaches the second cryptosync is used for verifying message

integrity by at least one of the two devices (Meandzija, Paragraph 0007,

communications between user terminal and access points). As established above in

the Response to Section B, Regarding Claim 1, a cryptosync can be a number of

cryptographic pieces of data including a digital certificate. A digital certificate is an

electronic document which uses a digital signature to bind a public key with an identity

information such as the name of a person or an organization, their address, and so

forth. The certificate can be used to verify that a public key belongs to an individual.

The individual in this case would be a user a terminal. Therefore it reads on the claimed

limitation of verifying the message integrity by at least one of the two devices, this

instance the device of the user terminal is being verified by the digital certificate it uses).

Response to Section B, Regarding Claims 6 and 11:

Appellant argues that Meandzija in view of Malcolm fail to disclose, teach or even suggest "deriving step derives the first cryptosync as at least a portion of the second cryptosync," regarding claims 6 and 11. Examiner respectfully disagrees. Meandzija in view of Malcolm teaches deriving step derives the first cryptosync as at least a portion of the second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate).

As established above in the Response to Section B, Regarding Claim 1, a cryptosync or in this case a digital certificate is taught by Malcolm to be derived from a root certificate. The definition of the word derive, is to obtain from a source, therefore if the first digital certificate is derived from the second digital certificate, then it must have at least a portion of the second digital certificate, since it has to be able to trace back to the source.

Response to Section B, Regarding Claims 7 and 12:

Appellant argues that Meandzija in view of Malcolm fail to disclose, teach or even suggest "the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence," regarding claims 7 and 12. Examiner respectfully disagrees. Meandzija in view of Malcolm teaches the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence (Malcolm, Paragraph 0145, certificate derived from root certificate).

As established above in the Response to Section B, Regarding Claim 6 and 11, a

certificate derived from a root will have information that traces back to the root

certificate/source. This would include fixed bit sequence, a fixed bit sequence can be a

number of things, one such interpretation is a public key bit length. The digital

certificates being used in the Malcolm and Meandzija are also known as public key

certificates. This would mean that all the digital certificates would be based off of a key

of a certain fixed length, thus all certificates derived from the root certificate would be of

the same bit length.

Response to Section C, Regarding Claims 2 and 3:

Appellant argues that Meandzija in view of Malcolm and Burch fail to disclose,

teach or even suggest "the second cryptosync is used for message encryption by at

least one of the two devices," regarding claim 2. Examiner respectfully disagrees.

Meandzija in view of Malcolm teaches the second cryptosync is used for message

encryption by at least one of the two devices (Burch, Paragraphs 0004 and 0023,

certificate encrypts communications).

Examiner would like to note that Burch was never relied upon to teach a second

cryptosync or digital certificate. As stated above the term digital certificate is being used

to interpret a cryptosync. Burch teaches on paragraphs 0004 and 0023 that public key

digital certificates have the ability to encrypt communications. Therefore the combined

with Meandzija and Malcolm, teach that it is well known to one of ordinary skill in the art

to have the digital certificate, taught by Malcolm would have the ability to encrypt

messages which is the limitation recited in claim 2.

Arguments regarding claim 3, are responded with the same rationale used in

Response to Section B, Regarding Claim 4.

Response to Section D, Regarding Claim 5:

Appellant argues that Meandzija in view of Malcolm and Somin fail to disclose,

teach or even suggest "the second cryptosync changes between communication

sessions," regarding claim 5. Examiner respectfully disagrees. Somin teaches the

second cryptosync changes between communication sessions (Somin, Paragraph

0043, new root certificate needed). Appellant's argue that Somin fails to identify where

Somin teaches a new group certificate. Somin on paragraph 0038, teaches the ability

of a new group root certificate being in the even that a new group is created. The group

root certificate is the second cryptosync and in combination with Somin teaches the

ability that a cryptosync can change which includes between communication sessions if

need be, therefore the combination of Meandzija in view of Malcolm and Somin teaches

the limitations of claim 5.

Response to Section E, Regarding Claim 8:

Appellant argues that Meandzija in view of Malcolm and Rezaiifar fails to

disclose, teach or even suggest "the deriving step derives most significant bits of the

first cryptosync as the portion of the second cryptosync and derives least significant bits

of the first cryptosync as the fixed bit sequence," regarding claim 8. Examiner

respectfully disagrees. Rezaiifar teaches the deriving step derives most significant bits

of the first cryptosync as the portion of the second cryptosync and derives least

significant bits of the first cryptosync as the fixed bit sequence (Rezaiifar, Col. 4 Lines

46 – 62, bit sequence). Rezaiifar teaches the ability to use least significant bits when

creating a crypto-sync.

Response to Section E, Regarding Claims 9, 10 and 13 – 23:

Appellant argues that it would not be obvious to have the combination of

Meandzija in view of Malcolm and Rezaiifar. Examiner respectfully disagrees. In

response to appellant's argument that there is no teaching, suggestion, or motivation to

combine the references, the examiner recognizes that obviousness may be established

by combining or modifying the teachings of the prior art to produce the claimed

invention where there is some teaching, suggestion, or motivation to do so found either

in the references themselves or in the knowledge generally available to one of ordinary

skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re*

Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v.*

Teleflex, Inc., 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, both the Meandzija,

Malcolm and Rezaiifar are analogous art. Rezaiifar teaches the use of cryptosyncs

which are used with encryption keys to encrypt communications. Meandzija teaches

the use of session certificates, which are valid for one communication session, to

connect a user terminal and a network access point. In combination the advantage of having a more secure communication session would exist.

Regarding claims 9, 10 and 13, Appellant argues that Meandzija in view of Malcolm and Rezaiifar, fail to disclose, teach or even suggest, "the fixed bit sequence is a string of 0s," regarding claims 9, 10 and 13. Examiner respectfully disagrees. Meandzija as modified teaches the fixed bit sequence is a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero). It has already been established in Response to Section E, Regarding Claim 8, that Rezaiifar teaches the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence. The fixed bit sequence being all zeros is not a positive step and is still a step the system would be capable of doing without needing to add a positive step.

Regarding claims 16 and 17, Appellant argues that Meandzija in view of Malcolm and Rezaiifar, fail to disclose, teach or even suggest, "teaches the deriving step is performed at a base station" and "teaches the deriving step is performed at a mobile station," regarding claims 16 and 17. Examiner respectfully disagrees Meandzija as modified teaches the deriving step is performed at a base station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations). Meandzija as modified teaches the deriving step is performed at a mobile station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations). Meandzija in view of Malcolm and Rezaiifar, teach that the secure communications between base stations and mobile devices. As responded to

above Malcolm teaches the derivation of a second cryptosync, this is capable of being done by the Certificate authorities described in paragraph 0145 of Malcolm.

Regarding claims 18, Appellant argues that Meandzija in view of Malcolm and Rezaiifar, fail to disclose, teach or even suggest, "encrypting a frame of information to send from the at least one of the two devices using the first cryptosync," regarding claim 18. Examiner respectfully disagrees. Meandzija as modified teaches encrypting a frame of information to send from the at least one of the two devices using the first cryptosync (Rezaiifar, Col. 2 Lines 19 – 23, encryption). Similar to rationale from Response to Section C, Regarding Claims 2 and 3, but with the Rezaiifar reference. Rezaiifar teaches on Col. 2 Lines 19 – 23, encryption of communications. Therefore the combined with Meandzija and Malcolm, teach that it is well known to one of ordinary skill in the art to have the digital certificate, taught by Malcolm would have the ability to encrypt messages

Regarding claims 20 and 23, Appellant argues that Meandzija in view of Malcolm and Rezaiifar, fail to disclose, teach or even suggest, "incrementing the first cryptosync after the encrypting step," regarding claims 20 and 23. Examiner respectfully disagrees. Meandzija as modified teaches incrementing the first cryptosync after the encrypting step (Rezaiifar, Col. 2 Lines 38 - 48, incrementing). It is clear the Rezaiifar teaches this limitation in the reference thus teaching the recited limitation of claim 20.

Regarding claims 21, Appellant argues that Meandzija in view of Malcolm and Rezaiifar, fail to disclose, teach or even suggest "decrypting a frame of information received at the at least one of the two devices using the first," regarding claim 21.

Examiner respectfully disagrees. Meandzija as modified teaches decrypting a frame of

information received at the at least one of the two devices using the first cryptosync

(Rezaiifar, Col. 5 Lines 56 – 67, decryption). Therefore the combined with Meandzija

and Malcolm, teach that it is well known to one of ordinary skill in the art to have the

digital certificate, taught by Malcolm would have the ability to decrypt messages

Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et

al. U.S. PG-Publication No. (2004/0078334) and Burch et al. U.S. PG-Publication No.

(2005/0172116).

As per claim 24, Meandzija teaches the first cryptosync having a life limited to the

communication session, the communication session being defined as a period of time a

channel for communication exists between the two communication devices (Meandzija,

Paragraph 0073, session certificate which is only valid for a single session) but fails to

teach deriving, at a network element, a value of a first cryptosync for the communication

session based on a value of a second cryptosync and the second cryptosync having a

life extending over multiple communication sessions and [cryptosync] used to encrypt

further communication between the two devices. However, in an analogous art Malcolm

teaches deriving, at a network element, a value of a first cryptosync for the

communication session based on a value of a second cryptosync (Malcolm, Paragraph

0145, certificate derived from root certificate) and the second cryptosync having a life

extending over multiple communication sessions (Malcolm, Paragraph 0145, certificate

derived from root certificate, the root certificate is being interpreted to be the second

cryptosync which will last over multiple sessions since all the signed certificates will

stem from the root) and Burch teaches [cryptosync] used to encrypt further

communication between the two devices (Burch, Paragraphs 0004 and 0023, certificate

encrypts communications).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Malcolm's Information management system Meandzija's

digital certificate related to the user terminal hardware in a wireless network because it

offers the advantage of ensuring that the transmission of data by their staff is always

carried out securely (Malcolm, Paragraph 0028).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Burch's techniques for dynamically establishing and

managing trust relationships with Meandzija's digital certificate related to the user

terminal hardware in a wireless network because it offers the advantage of improving

trust relationships (Burch, Paragraph 0008).

Response to Section F, Regarding Claims 24:

Please refer to rational used in Response to Section B, Regarding Claim 1

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Roderick Tolentino/

Examiner, Art Unit 2439

Conferees:

/Christian LaForgia/

Primary Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439